(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103404076 B
(45)授权公告日 2016.05.04

(21)申请号 201180068791.6
(22)申请日 2011.12.22
(30)优先权数据
1061367 2010.12.30 FR
(85)PCT国际申请进入国家阶段日
2013.08.30
(86)PCT国际申请的申请数据
PCT/FR2011/053143 2011.12.22
(87)PCT国际申请的公布数据
WO2012/089967 FR 2012.07.05
(73)专利权人 法国电信公司
地址 法国巴黎
(72)发明人 B. 米考 M. 罗布肖
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 李芳华
(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
US 5790667 A,1998.08.04,
US 7096494 B1,2006.08.22,
CN 100388852 C,2008.05.14,
US 2008208753 A1,2008.08.28,

审查员 裴广坤

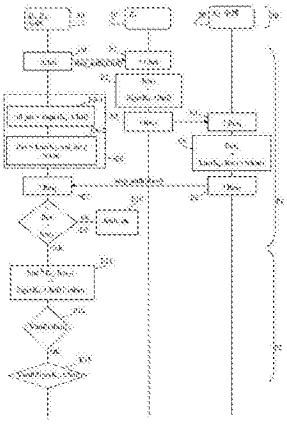
权利要求书2页 说明书8页 附图2页

(54)发明名称

在第三实体上认证第一和第二实体的方法

(57)摘要

本发明涉及在第三实体上对第一和第二实体进行认证的方法，所述第一和第三实体共享第一私钥，所述第二和第三实体共享第二私钥，该方法包括下列步骤：- 由第三实体向第一实体分派询问，- 由第一实体通过认证值的第一私匙的计算，- 由第一实体向第二实体分派认证值，- 由第二实体通过认证响应的第二私钥的计算，- 由第二实体向第三实体分派认证响应，- 期望认证响应的第三实体的计算，- 接收到认证响应与计算的期望认证响应的比较。



CN 103404076 B

1.一种通过第三实体(30)对第一实体(10)和第二实体(20)进行认证的方法,所述第一和第三实体共享第一私钥(K_1),所述第二和第三实体共享第二私钥(K_2),其中,该方法包括下列步骤:

-第三实体向第一实体发送(E0)询问(Cha1),

-第一实体基于接收到的询问使用第一私钥来计算(E2)认证值(Res_1),

-第一实体向第二实体发送(E3)所计算的认证值,

-基于对于第三实体和第二实体已知的令牌并基于从第一实体接收的认证值,第二实体使用以第二私钥作为参数的加密算法来计算(E5)认证响应(Res_2),

-第二实体向第三实体发送(E6)认证响应,

-基于令牌和询问,第三实体使用第一和第二私钥来计算(E8)期望认证响应(Res),

-将接收到的认证响应与所计算的期望认证响应进行比较(E9)。

2.如权利要求1所述的方法,其中,所述令牌包含多个填充比特。

3.如权利要求1所述的方法,其中,所述令牌包含询问的部分。

4.一种通过第三实体对第一和第二实体进行认证的方法,所述第一和第三实体共享第一私钥(K_1),所述第二和第三实体共享第二私钥(K_2),其中,该方法包括下列步骤:

-向第一实体发送(E0)询问(Cha1),

-基于对于第三实体和第二实体已知的令牌,使用以第二私钥作为参数的加密算法来计算(E8)期望认证响应(Res),且使用第一私钥来计算用于该询问的签名,

-从第二实体接收(E7)所述询问的响应(Res_2),

-将接收到的响应与所计算的认证响应进行比较(E9)。

5.如权利要求4所述的方法,其中,所述令牌包含多个填充比特。

6.如权利要求4所述的方法,其中,所述令牌包含询问的部分。

7.一种用第三实体(30)对由至少两个实体(10、20)构成的组进行认证的方法,该第三实体与组中的第一实体(10)共享第一私钥(K_1),第三实体与组中的第二实体(20)共享第二私钥(K_2),其中,所述方法包括下列步骤:

-从中心实体接收(E1)询问,

-基于接收到的询问,组中的第一实体使用第一私钥来计算(E2)认证值(Res_1),

-第一实体向组中的第二实体发送(E3)所计算的认证值,

-基于对于第三实体和第二实体已知的令牌并基于从第一实体接收的认证值,组中的第二实体使用以第二密钥作为参数的加密算法来计算(E5)认证响应(Res_2),

-组中的第二实体向第三实体发送(E6)所计算的认证响应。

8.如权利要求7所述的方法,其中,所述令牌包含多个填充比特。

9.如权利要求7所述的方法,其中,所述令牌包含询问的部分。

10.一种适于对第一和第二实体进行认证的认证装置(30),所述装置与第一实体共享第一密钥(K_1),并与第二实体共享第二密钥(K_2),其中,所述装置包括:

-发送装置(304),被设计为将询问(Cha1)发送到第一实体,

-计算装置(305),被设计为基于对于认证装置和第二实体已知的令牌,使用以第二密钥作为参数的加密算法来计算期望认证响应(Res),并使用第一密钥来计算所述询问的签名,

-接收装置(306),被设计为从所述第二实体接收对于所述询问的响应(Res_2),

-比较装置(307),被设计为将接收到的响应与所计算的认证响应进行比较。

11.一种包含第一和第二实体的两个实体的集合,所述集合适于通过如权利要求10所述的认证装置来认证,该认证装置与第一实体共享第一密钥(K_1),并与第二实体共享第二密钥(K_2),其中,所述集合包括:

-接收装置(404),被设计为从认证装置接收询问,

-第一计算装置(405),被设计从而组中的第一实体基于询问使用第一密钥来计算认证值(Res_1),

-传输装置(406),被设计从而第一实体将认证值传输到组中的第二实体,

-第二计算装置(407),被设计从而第二实体基于对于认证装置和第二实体已知的令牌并基于从集合中的第一实体接收的认证值,使用以第二密钥作为参数的加密算法来计算认证响应(Res_2),

-发送装置(408),被设计为向认证装置发送所计算的认证响应。

12.一种认证系统,包括:

-如权利要求10所述的认证装置,以及

-如权利要求11所述的两个实体的集合。

在第三实体上认证第一和第二实体的方法

技术领域

[0001] 本发明涉及用第三实体来对至少两个分离的实体进行认证的方法。

[0002] 更准确地说，本发明允许通过通信信道与中心实体通信的多个实体的认证，其降低了带宽和交换的消息数。

背景技术

[0003] 本发明尤其可被有利地用于移动电信的领域，特别是运营商希望对“SIM”卡或“USIM”卡(“(通用)用户身份识别卡”)类型的装置或装载该卡的终端进行认证的情况。这样的认证使其可以确保卡和终端关联并且只能被一起使用。该情形更加令人关注，因为研发了越来越多的设备来使用移动网络而没有物理用户处理该设备的安全性。例如，这是具有网络设备的情况，例如具有“LTE”(“长期演进”)中继的情形，其旨在扩展无线网络而同时以和移动终端类似的方式来运行，或者“M2M”(“机器到机器”)设备，例如，其被用于远程维护应用或远程报警应用。

[0004] 通过示例，在一台M2M设备上安装的M2M应用使用移动运营商网络，以允许中心用户与该设备远程地交换信息，以采集该设备上存储的信息或修改其状态而无人工干涉且特别是没有对M2M设备的连续人工监视。为了针对移动网络来实现这些信息的交换，向该设备提供USIM卡类型的卡。通过与移动用户终端类似的方式，M2M设备经历来自网络的认证。更准确地说，基于已知的认证算法由网络对USIM卡进行认证。但是，在目前的网络认证过程中，与USIM卡关联的移动设备未被网络或USIM卡认证。于是，它不能被移动网络设施人为是可信的设备。

[0005] 已经有建议来克服该问题。通过示例，3GPP文档http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_61_Sorrento/DOcs/S3-101404.zip提出了一种对与移动终端关联的USIM卡进行认证的方案，该USIM卡被插入到移动终端中。基于该方案，网络和USIM卡以传统的方式来共享认证密钥K，且网络和终端共享对称密钥$K_{terminal}$。由此根据下列步骤来执行认证：

[0006] -网络以传统的方式向USIM卡发送RAND询问，

[0007] -USIM卡通过将已知的认证算法F2应用到以密钥K作为参数的RAND询问来计算响应；它将该响应发送到终端，

[0008] -终端使用属于终端$K_{terminal}$的对称密钥来计算该响应的签名，以产生对RAND询问的新响应，

[0009] -将该新响应发送到网络，

[0010] -网络于是可以通过验证接收到的响应的签名来对终端和USIM卡进行认证，并同样对响应进行认证。

[0011] 但是，在网络认证失败的情形下，该解决方案无法识别认证错误来自USIM卡还是终端或者来自两者。

发明内容

[0012] 本发明的目标是提出一种通过第三方实体对第一实体和第二实体进行认证的方法以改善该情形，所述第一和第三实体共享第一私钥，所述第二和第三实体共享第二私钥，其中，该方法包括下列步骤：

[0013] -第三实体向第一实体发送询问，

[0014] -第一实体基于接收到的询问使用第一私钥来计算认证值，

[0015] -第一实体向第二实体发送所计算的认证值，

[0016] -基于第三实体和第二实体已知的令牌并基于从第一实体接收的认证值，第二实体使用以第二私钥作作为参数的加密算法来计算认证响应，

[0017] -第二实体向第三实体发送认证响应，

[0018] -基于令牌和询问，第三实体使用第一和第二私钥来计算期望认证响应，

[0019] -将接收到的认证响应与所计算的期望认证响应进行比较。

[0020] 于是，根据本发明的方法允许同一认证操作期间通信的两个不同实体的认证。两个认证的实体由此被关联，在于其认证是通过第三实体来共同执行的。

[0021] 于是，该认证使其可以确保认证的实体一起运行。通过示例，在移动网络中(在该网络中第一实体是SIM卡或USIM卡，且第二实体是(U)SIM卡所插入的终端)的两个实体认证的情形下，认证使其可以确保(U)SIM卡确实已被插入到移动终端中并仅和终端一起运行。该方面关注在没有人工监视的M2M设备或LTE中继的情形下的安全性。

[0022] 此外，本发明的方法使其可以重新使用最初为单个实体的认证而定义的通信信道和接口。于是不需要修改接口或定义负责认证的第三实体和两个认证实体之间的新消息。例如，该方面关心移动网络中的两个实体进行认证的情形。这是因为，开发网络中的接口将是长期的工作。一般来说，该方法最小化在负责认证的第三实体和要被认证的两个实体之间交换的消息，因为在第三实体和两个实体之间交换的消息数量等于认证单个实体时交换的消息数量。

[0023] 此外，本发明使其可以在两个实体中的一个认证失败时识别两个中哪一个失败了。首先通过用于认证的加密算法的使用且其次通过在要认证的实体和第三实体之间各自私钥以及第二和第三实体已知的令牌的共享，该方面变得可能。

[0024] 本发明还涉及一种通过第三实体对第一和第二实体进行认证的方法，所述第一和第三实体共享第一私钥，所述第二和第三实体共享第二私钥，其中，该方法包括下列步骤：

[0025] -向第一实体发送询问，

[0026] -基于对于第三实体和第二实体已知的令牌并基于询问，使用第一和第二密钥来计算期望认证响应，

[0027] -从第二实体接收对所述询问的响应，

[0028] -将接收到的响应与所计算的认证响应进行比较。

[0029] 本发明类似地涉及用第三实体对由至少两个实体构成的组进行认证的方法，该第三实体与组中的第一实体共享第一私钥，第三实体与组中的第二实体共享第二私钥，其中，所述方法包括下列步骤：

[0030] -从中心实体接收询问，

[0031] -基于接收到的询问，组中的第一实体使用第一私钥来计算认证值，

[0032] -第一实体向组中的第二实体发送所计算的认证值，

[0033] -基于对于第三实体和第二实体已知的令牌并基于从第一实体接收的认证值，组中的第二实体使用以第二密钥作为参数的加密算法来计算认证响应，

[0034] -组中的第二实体向第三实体发送所计算的认证响应。

[0035] 在一个示例性实施例中，如果接收到的认证响应不等于所计算的响应，则该方法类似地包括由第三实体实现的下列步骤：

[0036] -使用第二密钥对接收到的认证响应进行解密，

[0037] -验证所解密的响应包含令牌。

[0038] 如果验证是肯定的，则该方法类似地包括基于询问和第一密钥来计算期望值，并验证所解密的响应包含该期望值。

[0039] 因此，当认证失败时，方法允许已经失败的实体的精确识别。因此，在认证失败的时候，可以将认证错误归因于第二实体，或者如果第二实体已经正确地认证，则将认证错误归因于第一实体。

[0040] 在一个示例性实施例中，令牌包含多个填充比特。

[0041] 在另一示例性实施例中，令牌包含询问的一部分。

[0042] 在本发明的该实施例中，认证方法的安全性被提升，因为一次认证和另一次认证的令牌会变化。

[0043] 本发明类似地还涉及一种适于对第一和第二实体进行认证的认证装置，所述装置与第一实体共享第一密钥，并与第二实体共享第二密钥，其中，所述装置包括：

[0044] -发送装置，被设计为将询问发送到第一实体，

[0045] -计算装置，被设计为基于认证装置和第二实体已知的令牌、使用以第二密钥作为参数的加密算法来计算期望认证响应，并使用第一密钥来计算所述询问的签名，

[0046] -接收装置，被设计为从所述第二实体接收对所述询问的响应，

[0047] -比较装置，被设计为将接收到的响应与计算的认证响应进行比较。

[0048] 本发明还涉及包含第一和第二实体的两个实体的集合，所述集合适于通过根据本发明的认证装置来认证，该认证装置与第一实体共享第一密钥，并与第二实体共享第二密钥，其中，所述集合包括：

[0049] -接收装置，被设计为从认证装置接收询问，

[0050] -第一计算装置，被设计从而组中的第一实体基于询问使用第一密钥来计算认证值，

[0051] -传输装置，被设计从而第一实体将认证值传输到组中的第二实体，

[0052] -第二计算装置，被设计从而第二实体基于对于认证装置和第二实体已知的令牌并基于从集合中的第一实体接收的认证值，使用以第二密钥作为参数的加密算法来计算认证响应，

[0053] -发送装置，被设计为向认证装置发送所计算的认证响应。

[0054] 本发明还涉及一种认证系统，包括：

[0055] -根据本发明的认证装置，以及

[0056] -根据本发明的两个实体的集合。

[0057] 本发明类似涉及一种在数据存储介质上的计算机程序，并且能够被载入到认证装置的内部存储器中，该程序包含由装置执行的代码部分，当程序在所述装置上执行时，该代码部分用于执行认证方法的步骤。

[0058] 本发明还涉及一种数据存储介质，根据本发明的计算机程序被记录在该介质上。

附图说明

[0059] 参考以非限制的方式提供的附图阅读特定实施例的描述，本发明的多种细节和优势将被更好地理解，在附图中：

[0060] -图1描述了根据本发明的第一特定实施例的用第三实体来对两个实体进行认证的方法的步骤；

[0061] -图2描述了能够实现图1的方法的认证装置的特定例子；

[0062] -图3示出了能够实现图1的方法的两个实体的组的特定例子。

具体实施方式

[0063] 现在将参考图1来描述用第三实体对两个实体进行认证的方法。

[0064] 在同一认证操作中，可以通过第三实体30对第一实体10和第二实体20进行认证。在这里描述的实施例中，第三实体30是移动通信网络，诸如“GSM”(“全球移动通信系统”)网络或“GPRS”(“通用分组无线业务”)网络。在该情形下，例如，第三实体是网络中的认证中心。例如第一实体10是“SIM”卡或“USIM”(“通用用户身份识别卡”)卡类型的用户身份识别卡，且例如第二实体20是用户卡所插入的移动终端。

[0065] 在初始的配置阶段P0，定义接下来在用第三实体30对第一和第二实体10、20进行认证时要使用的特定数量的参数。配置阶段P0仅被执行一次。在配置阶段P0中，在第一实体10和第三实体30之间共享第一私钥K_1。同样，在第二实体20和第三实体30之间共享第二私钥K_2。此外，在该初始配置阶段P0，在第二实体20和第三实体30之间共享令牌的知识。令牌是数字数据项，其可以是固定的或可变的。令牌是第二实体20和第三实体30能够获取的数据项。通过示例，令牌对应于多个填充比特“0x00”。

[0066] 一旦配置阶段P0已被执行，就可以进行后续的认证阶段P1。只要需要就尽可能多次地执行认证阶段P1，以便第三实体30对第一和第二实体10、20进行共同认证。后续的步骤E0到E10描述了认证阶段P1。

[0067] 在用于发送认证请求的初始步骤E0中，第三实体30向第一实体10发送认证请求消息req_auth。认证请求消息包括询问Chal。询问Chal是由第三实体30对当前的认证阶段P1选择的随机值。由此在用于接收询问的步骤E1中由第一实体10来接收询问Chal。

[0068] 在用于计算认证值的步骤E2中，第一实体10基于询问Chal和与第三实体30共享的私钥K_1来计算认证值Res_1。通过示例，第一实体10通过将以所共享的第一私钥K_1作为参数的签名算法用于询问Chal来计算认证值。换句话说，$Res_1=Sign(K_1,Chal)$；其中，Sign是已知的签名算法，例如“MAC”(“消息认证码”)算法。在GSM网络的情形下，Sign是所使用的算法A3。在发送步骤E3中，由第一实体10向第二实体20传输认证值Res_1。

[0069] 在接收步骤E4中，第二实体20从第一实体10接收认证值Res_1。

[0070] 在用于计算认证响应的步骤E5中，第二实体20计算认证响应Res_2。为此，第二实体

20将以所共享的第二私钥K_2作为参数的加密算法Enc用于从第一实体10接收的认证值Res_1，并与令牌连接。令牌对于第三实体30和第二实体20来说是已知的。换句话说，$Res_2=Enc(K_2, Res_1||token)$；其中，Enc是已知的加密算法。通过示例，加密算法Enc为“AES”(“高级加密标准”)算法，或者“DES”(“数据加密标准”)算法。Res_2构成对初始步骤E0中由第三实体30发送的认证请求消息req_auth的响应。

[0071] 在用于发送响应的步骤E6中，第二实体20向第三实体30发送响应消息resp_auth，其包含在步骤E5中计算的认证响应Res_2。

[0072] 在接收步骤E7中，第三实体30从第二实体20接收响应消息resp_auth以及由此计算的认证响应Res_2。

[0073] 在用于计算期望响应的步骤E8中，第三实体30计算期望认证响应Res。为此，在步骤E8的子步骤E8-1中，第三实体30使用签名函数来计算中间值val_int，该签名函数和在步骤E2中由第一实体10应用于的签名函数相同。换句话说，第三实体通过将以所共享的第一私钥K_1作为参数的签名算法Sign用于询问Chal来计算$val_int=Sign(K_1,Chal)$。在后续的子步骤E8-2中，第三实体30通过应用加密算法来计算期望认证响应Res，该加密算法与步骤E5中由第二实体使用的加密算法相同。换句话说，第三实体30通过将以所共享的第二私钥K_2作为参数的加密算法应用于在前面的子步骤中获取的与令牌连接的中间值val_int，计算$Res=Enc(K_2,val_int||token)$。

[0074] 可以理解，用于计算期望结果的步骤E8可以由第一和第二实体10、20执行的步骤来独立地执行。于是，在该方法的另一实施例中，连续执行步骤E8到步骤E10用于发送询问。

[0075] 在比较步骤E9中，第三实体30将在步骤E8中计算的期望认证响应Res与在步骤E7中从第二实体20接收的认证响应Res_2进行比较。

[0076] 如果比较是肯定的(图1中的ok分支)，即如果所计算的认证响应Res等于从第二实体20接收的认证响应Res_2，则第一和第二实体的认证成功。由此在同一认证阶段中两个实体被正确地认证。第三实体30于是处于成功认证的状态E10。

[0077] 如果比较是否定的(图1中Nok分支)，则在分析阶段P2中执行分析，以便从第一实体10确定认证错误项是否来自第二实体，或者如果第二实体20是否成功认证。

[0078] 于是，在解密步骤E11中，第三实体30所使用所共享的私钥K_2对从第二实体20接收的认证响应Res_2进行解密。为此，第三实体12计算$Enc^{-1}(K_2,Res_2)$，其中，Enc^{-1}表示与加密算法Enc关联的解密算法。注意到，当认证成功时，解密的认证响应等于第一值和第二值的连接，该第一值对应于来自使用所共享的第一密钥K_1的询问Chal进行的签名，该第二值对应于令牌。换句话说，在成功认证的情形下，验证下列等式：

[0079] $Enc^{-1}(K_2,Res_2)=Sign(K_1,Chal)||token$

[0080] 注意到，由于令牌的大小对于第三实体30来说是已知的，所以第三实体30很容易区分第一和第二值。

[0081] 用于验证令牌的步骤E12验证对于第二和第三实体20、30已知的令牌是否确实等于所解密的认证响应所包含的第二值。如果验证是肯定的，则第二实体20被正确的认证。如果验证是否定的，即如果令牌未被包含在所解密的认证响应中，则第二实体20的认证失败。这是因为在该情形下，第二实体20未使用在配置阶段P0中同意的令牌，或者未使用正确的加密算法Enc，或者未使用所共享的第二密钥K_2。在这三种情形下，第二实体20的认证失败。

[0082] 如果在步骤E12中执行的令牌的验证是肯定的(图中的ok分支),即如果第二实体20的认证已经成功,于是,在后续的签名验证步骤E13中,第三实体30验证所解密的验证响应的第一部分。于是,第三实体30通过将以所共享的第一密钥K_1作为参数的签名算法Sign应用于询问Chal来计算期望值。换句话说,第三实体30计算Sign(K_1,Chal)。如果期望值不等于所解密的认证响应所包含的第一值,则第一实体10的认证失败了。

[0083] 注意到,在分析阶段P2中,可将认证错误归因于第二实体20,或者如果第二实体20的认证成功,则归因于第一实体10。

[0084] 这里在(U)SIM卡的通过GSM或GPRS网络进行认证的背景中描述本发明,该(U)SIM卡与插入该卡的移动终端关联。当然,本发明不限于这些网络。于是,该方法类似地应用于其他网络中的认证,例如"UMTS"("通用移动电信系统")网络。在该例子中,由第一实体10为了计算认证值而实现的签名算法由此是"AKA"("认证密钥协商")算法。

[0085] 同样,该方法不限于对移动网络的(U)SIM卡和终端进行认证。更一般来说,该方法应用于通过第三实体对两个通信实体进行的认证。于是,在另一示例性实施例中,通过网络对(U)SIM卡和移动终端外部的实体(例如附接到要购买的产品商的"RFID"("无线射频识别")组件)共同进行认证。在该情形下,终端适于在RFID标签读取器模式下运行。(U)SIM卡和标签能够经由移动终端来通信。于是,(U)SIM卡和RFID标签的共同认证可对应于收据的安全获取,该收据通过终端来验证产品的购买。在使用的另一情形下,第二实体与外部装置(例如合并"NFC"("近场通信")组件的停车计时器)关联。终端作为NFC终端的一部分,并且网络对U(SIM)卡和作为NFC卡的停车计时器的共同认证对使用终端对停车票的购买进行验证。

[0086] 一般认为,在配置阶段P0中,密钥K_1、K_2被分别分发到第一和第二实体10、20,每一个密钥与第三实体30共享。在这里针对移动网络描述的例子中,第一实体是(U)SIM卡且第二实体是卡所插入的终端。一般被称为认证密钥的第一密钥K_1在制造卡的步骤中被定义并且安装在(U)SIM卡中。一旦设备已进入流通,第二密钥K_2就可被安装在终端上。该安装可以例如使用公钥密码系统以安全的方式来实现,该公钥密码系统在终端制造期间设置的并且意图允许来自第三实体或者来自分发密钥的专门实体的所共享的第二私钥K_2的安全安装。在该情形下,用于分发密钥的实体然后将所共享的第二密钥K_2分发到第二和第三实体20、30。

[0087] 对第二和第三实体20、30已知的令牌可以是固定的。通过示例,如前所述,它可以由填充比特"0x00"构成。在另一示例性实施例中,令牌可以是可变的,且对应于在认证阶段开始时发送的询问Chal的部分。在该情形下,第三实体30和第二实体20在配置阶段P0同意询问的哪一部分对应于令牌。通过示例,构成令牌的询问的前x比特、最后x比特、前x个最高位等对应于令牌。

[0088] 令牌的大小需要被调整,从而认证的安全性与由第二实体20传输的认证结果的最大授权大小具有可比性。于是,在与第三代移动网络(其中认证结果一般在32和128比特之间)中的认证对应的一个示例性实施例中,具有32和64比特之间的大小的令牌显得合理。于是,认证响应具有64和96比特之间的大小。另一方面,为了与由网络提供的无线接口的兼容性,由第一实体(在该情形下是(U)SIM卡)所计算的认证响应Res_1可被裁剪。通过示例,当(U)SIM卡被配置为产生128比特的认证值Res_1时,并且当与网络的无线接口由此适于传输

该响应时，显得需要裁剪由(U)SIM卡产生的认证值以便将令牌计入考虑。原因在于，与第二实体20，在该情形下是终端的认证值Res_1与令牌进行连接。于是，在该例子中，第一实体10可将认证值Res_1裁剪至64或96比特，这使其可以使用64或32比特的令牌。当然，在该情形下，在用于计算期望响应的步骤E8中，第三实体30，在该情形下是网络，类似地对它计算的中间值val_int进行裁剪。

[0089] 现在将参考图2来描述能够实现图1的方法的认证装置30的特定例子。认证装置30(图2中未示出)能够认证至少两个实体的组。通过示例，认证装置30是在与通过网络对两个实体进行的认证相关的方法的情形下用于移动网络的认证服务器。在另一示例性实施例中，认证装置是能够对U(SIM)卡和终端外部的实体进行认证的移动终端。

[0090] 在所有这些情形下，认证装置包括：

[0091] -处理器301，或“CPU”(“中央处理单元”)，或处理单元。处理器301链接到一组存储器：

[0092] -随机存取存储器302，或“RAM”，允许计算、指令载入及其执行的进行，

[0093] -只读存储器303，或非易失性存储器，或“ROM”，适于存储非易失性数据，例如加密算法。于是，存储器303存储签名算法Sign和加密算法Enc。它类似地存储令牌，或允许获取所述令牌的方法。存储器303类似地适于在保护区域中存储认证装置与要认证的实体所共享的私钥。通过示例，存储器存储与要认证的第一实体共享的第一私钥K_1以及与要认证的第二实体共享的第二私钥K_2。

[0094] 认证装置30类似地以程序的形式来容纳应用，该程序能够实现由装置执行的本发明的方法的步骤。为此，装置30类似的包括：

[0095] -发送装置304，被设计为向要认证的第一实体发送包含询问Chal的认证请求消息，

[0096] -计算装置305，被设计为计算期望认证响应Res。为此，在运行期间，装置30将以所存储的第二密钥K_2作为参数的加密算法Enc应用到将第一值与令牌连接而获得的数据项。通过将以第一共享密钥K_1作为参数的签名算法应用到询问Chal来获得该第一值。计算装置305适于实现前述认证方法的用于计算期望响应的步骤E8。

[0097] -接收装置306，被设计为从第二实体接收由发送装置304发送的认证请求的响应消息用于询问。接收装置306被设计为实现前述认证方法的接收步骤E7，

[0098] -比较装置307，被设计为将从第二实体接收的认证响应与由计算装置305计算的认证结果进行比较。比较装置307适于实现前述的认证方法的比较步骤E9，

[0099] -分析装置308，被设计为识别由比较装置307检测到的认证错误的来源。分析装置308包括：

[0100] -解密装置308-1，被设计为使用所共享的第二私钥K_2对从第二实体接收的认证响应Res_2进行解密。解密装置308-1适于实现认证方法的解密步骤E11，

[0101] -用于验证令牌的装置308-2，被设计为验证对于认证装置30已知的令牌被包含在由解密装置308-1所解密的认证响应中。装置308-2适于实现前述认证方法的用于验证令牌的步骤E12，

[0102] -签名验证装置308-3，被设计为使用以第一私钥K_1作为参数的Sign算法来验证所解密的认证响应的第一部分确实符合询问的签名。装置308-3适于实现前述认证方法的签

名验证步骤E13。

[0103] 发送装置304、计算装置305、接收装置306、比较装置307、包含解密装置308-1、验证令牌的装置308-2以及签名验证装置308-3的分析装置308优选地是包含软件指令的软件模块，该软件指令用于使用认证装置30来执行前述方法的步骤。软件模块可被存储在数据存储介质中或通过数据存储介质来传输。后者可以是硬件存储介质，例如CD-ROM、磁存储器，或者传输介质例如信号或电信网络。

[0104] 现在将参考图3来描述适于被前述认证装置30认证的两个实体的集合40的特定例子。

[0105] 集合40包括第一实体和第二实体，在图3中没有示出。

[0106] 实体的集合包括：

[0107] -处理单元401，或CPU。可以理解，两个实体中的每一个都具有其自己的处理单元。在图3中用处理单元401来表示该CPU集合。该处理单元链接到多个存储器：

[0108] -随机存取存储器402，或RAM存储器，适于允许计算的进行、指令的载入以及后面的执行。再一次这里可以理解，每一个实体具有其自己的RAM存储器。用存储器402来表示这些RAM存储器的集合，

[0109] -非易失性存储器403，或ROM存储器，适于存储非易失性数据例如密码算法。可以理解，每一个实体具有这样的存储器。但是，用单个ROM存储器403来表示实体的存储器的集合。存储器403存储加密算法，特别是适于计算认证值的签名算法Sign，以及适于计算认证响应Res_2的加密算法Enc。它还存储令牌，或者允许获取该令牌的方法。存储器403类似地在安全区域中存储与认证装置所共享的私钥。特别地，它存储所共享的第一私钥K_1和所共享的第二私钥K_2，

[0110] -接收装置404，其被设计为从认证装置接收包含询问的认证请求消息。接收装置404实现前述认证方法的用于接收询问的步骤E1，

[0111] -第一计算装置405，被设计从而集合中的第一实体使用签名算法Sign来用第一密钥K_1来计算认证值Res_1，该签名算法Sign被应用于由接收装置404接收的询问。第一计算装置405适于实现本发明的方法的用于计算认证值的步骤E2，

[0112] -传输装置406，其被设计从而第一实体将由计算装置405计算的认证值发送到集合中的第二实体。发送装置406适于实现认证方法的用于发送认证值的步骤E3，

[0113] -第二计算装置407，其被设计从而第二实体通过将以第二密钥K_2作为参数的加密算法Enc应用到由集合中的第一实体所计算的认证值来计算认证响应Res_2。第二计算装置407适于实现前述方法的用于计算认证响应的步骤E5，

[0114] -发送装置408，其被设计为向认证装置发送响应消息，该响应消息包含由第二计算装置407所计算的认证响应。发送装置适于实现用于发送认证响应的步骤E6。

[0115] 接收装置404、第一计算装置405、发送装置406、第二计算装置407和发送装置408优选地是包含软件指令的软件模块，该软件指令用于使用由两个实体构成的集合来执行前述方法的步骤。软件模块可被存储在数据存储介质中或通过数据存储介质来发送。后者可以是硬件存储介质，例如CD-ROM、磁存储器，或甚至是传输介质例如信号或电信网络。

[0116] 本发明还涉及一种认证系统，其包含认证装置30以及至少两个实体的集合40。

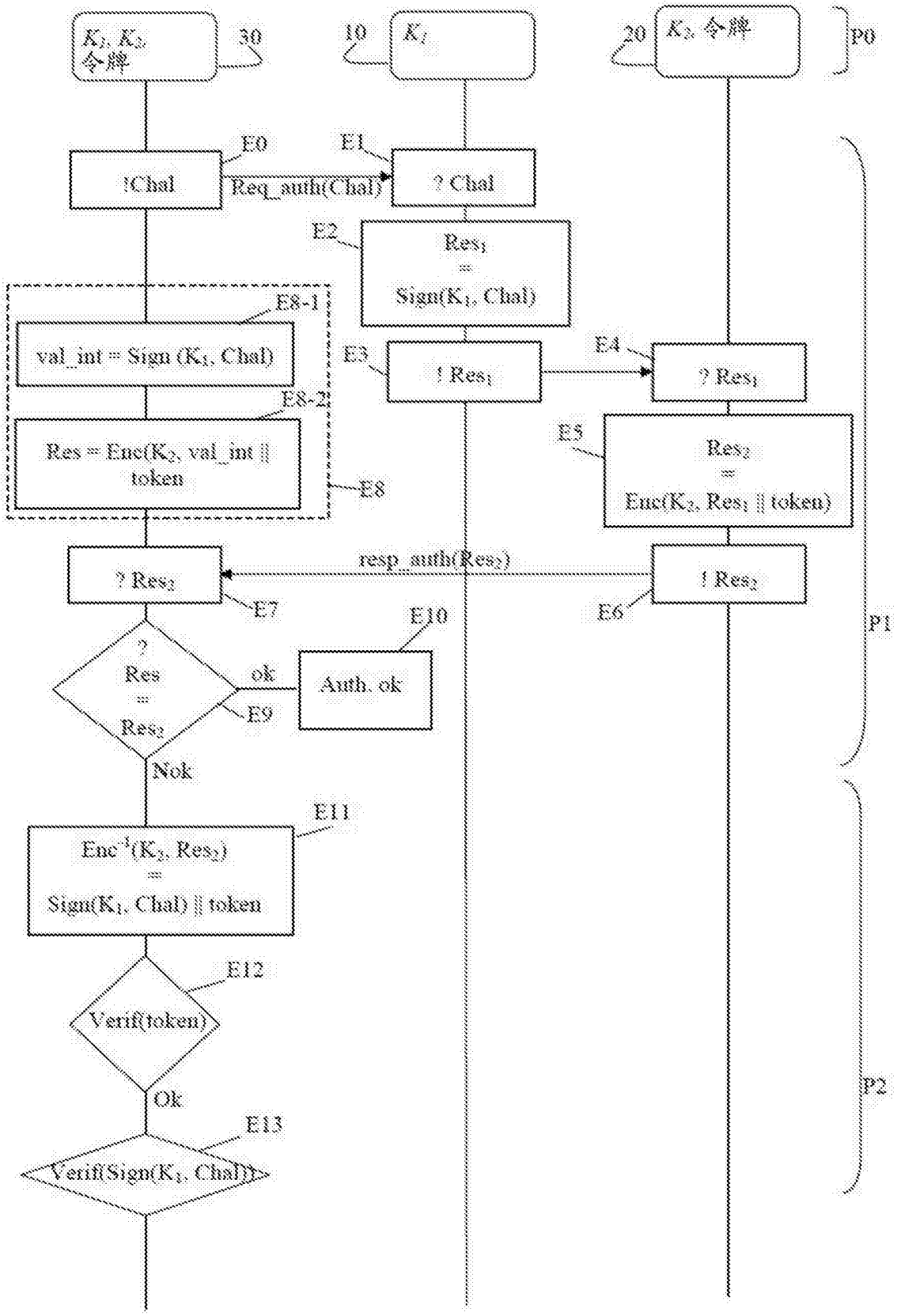

K1, K2, 令牌
30
10
K1
20
K2, 令牌
P0
E0
!Chal
Req_auth(Chal)
E1
? Chal
E2
Res1 = Sign(K1, Chal)
E8-1
val_int = Sign (K1, Chal)
E3
! Res1
E4
? Res1
E8-2
Res = Enc(K2, val_int || token
E8
E5
Res2 = Enc(K2, Res1 || token)
? Res2
resp_auth(Res2)
! Res2
E7
E6
P1
E10
?
Res
=
Res2
ok
Anth. ok
E9
Nok
E11
Enc-1(K2, Res2) = Sign(K1, Chal) || token
E12
Verif(token)
Ok
E13
Verif(Sign(K1, Chal))
P2

图1

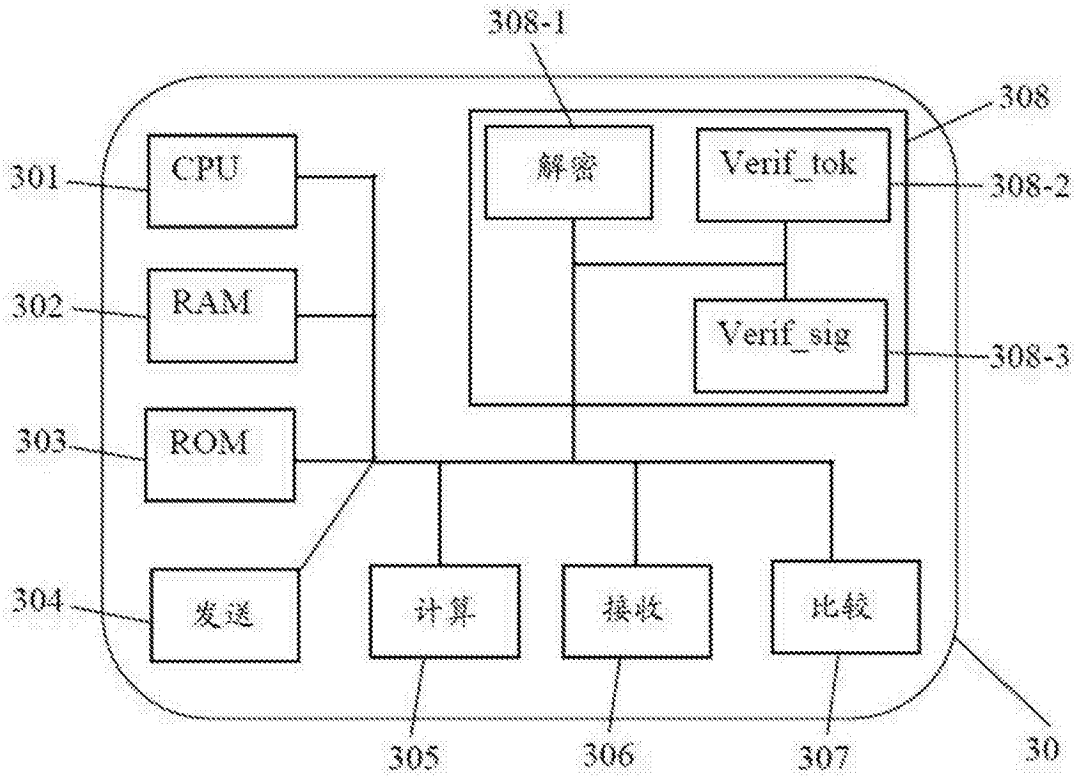

308-1
308
301
CPU
解密
Verif_tok
308-2
302
RAM
Verif_sig
308-3
303
ROM
304
发送
计算
接收
比较
305
306
307
30

图2

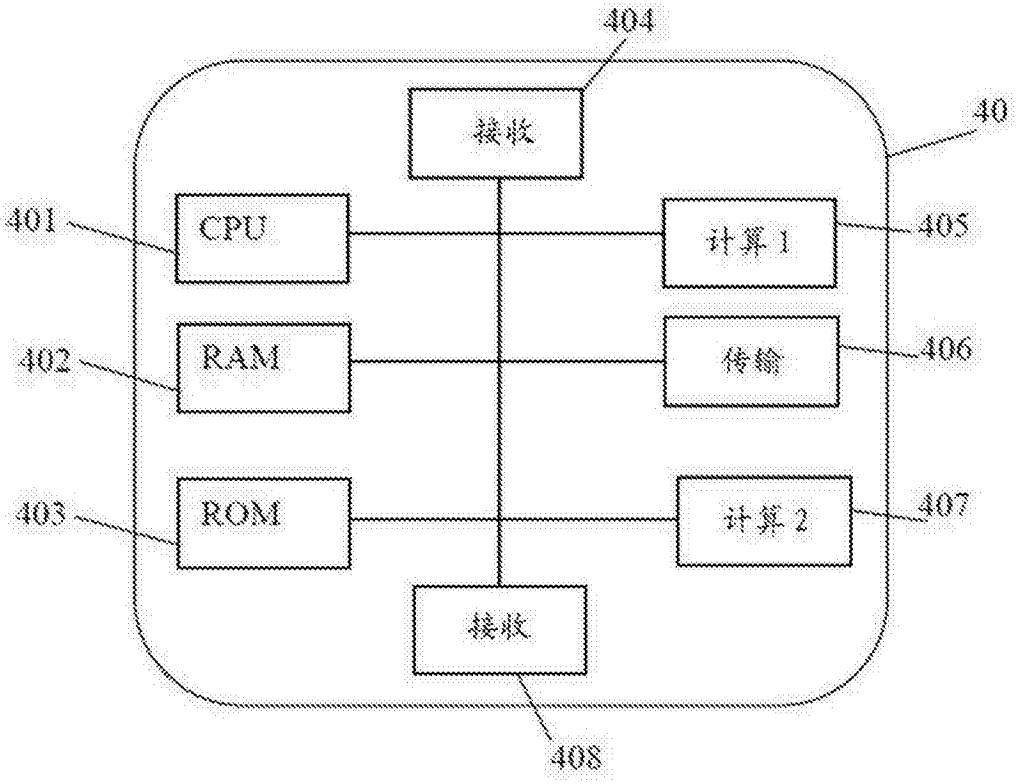

404
接收
40
401
CPU
计算 1
405
402
RAM
传输
406
403
ROM
计算 2
407
接收
408

图3